IN THE CLAIMS

Amended claims follow:

1. (Currently Amended) A computer program product stored on a computer-readable medium for controlling a computer to scan data accessible via an internet link for malware, said computer program product comprising:

(i) address identifying code operable to identify within currently held data at least one internet address associated with said currently held data;

(ii) retrieving code operable to pre-emptively retrieve via said internet link addressed data that would be accessed by a user following said at least one internet address; ~~and~~

(iii) scanning code operable to scan said addressed data for malware; and

(iv) storing code operable to store result data identifying at least addressed data in which malware was not found;

wherein said addressed data is cached when it has been retrieved.

2. (Cancelled)

3. (Original) A computer program product as claimed in claim 1, wherein said address identifying code is operable to search within said currently held data for string data having a format matching a pointer to an internet address.

4. (Original) A computer program product as claimed in claim 1, wherein said currently held data includes received e-mail messages.

5. (Original) A computer program product as claimed in claim 1, wherein said scanning code is operable to seek to detect within said addressed data one or more of:

computer viruses;

worms;

Trojans;

banned computer programs;
banned words; or
banned images.

6. (Original) A computer program product as claimed in claim 1, wherein said computer is a firewall computer via which internet traffic is passed to a local computer network.

7. (Cancelled)

8. (Original) A computer program product as claimed in claim 1, wherein if malware is detected within said addressed data, then one or more malware found actions are triggered.

9. (Previously Presented) A computer program product as claimed in claim 1, wherein said malware found actions including at least one of:

(i) preventing access to said currently held data;

(ii) removing said at least one internet address from said currently held data;

(iii) preventing access to said addressed data;

(iv) removing said malware from said addressed data to generate clean addressed data and supplying said clean addressed data in place of said addressed data;

(v) blocking internet access by a computer detected to be seeking to access said at least one internet address.

10. (Currently Amended) A method of scanning data accessible via an internet link for malware, said method comprising the steps of:

(i) identifying within currently held data at least one internet address associated with said currently held data;

(ii) pre-emptively retrieving via said internet link addressed data that would be accessed by a user following said at least one internet address; ~~and~~

(iii) scanning said addressed data for malware; and

(iv) storing result data identifying at least addressed data in which malware was not found;

wherein said addressed data is cached when it has been retrieved.

11. (Cancelled)

12. (Original) A method as claimed in claim 10, wherein said step of identifying includes searching within said currently held data for string data having a format matching a pointer to an internet address.

13. (Original) A method as claimed in claim 10, wherein said currently held data includes received e-mail messages.

14. (Original) A method as claimed in claim 10, wherein said step of scanning seeks to detect within said addressed data one or more of:

computer viruses;
worms;
Trojans;
banned computer programs;
banned words; or
banned images.

15. (Original) A method as claimed in claim 10, wherein said method is performed by a firewall computer via which internet traffic is passed to a local computer network.

16. (Cancelled)

17. (Original) A method as claimed in claim 10, wherein if malware is detected within said addressed data, then one or more malware found actions are triggered.

18. (Original) A method as claimed in claim 10, wherein said malware found actions including at least one of:

(i) preventing access to said currently held data;

(ii) removing said at least one internet address from said currently held data;

(iii) preventing access to said addressed data;

(iv) removing said malware from said addressed data to generate clean addressed data and supplying said clean addressed data in place of said addressed data;

(v) blocking internet access by a computer detected to be seeking to access said at least one internet address.

19. (Currently Amended) Apparatus for scanning data accessible via an internet link for malware, said apparatus comprising:

(i) address identifying logic operable to identify within currently held data at least one internet address associated with said currently held data;

(ii) retrieving logic operable to pre-emptively retrieve via said internet link addressed data that would be accessed by a user following said at least one internet address; ~~and~~

(iii) scanning logic operable to scan said addressed data for malware; and

(iv) storing logic operable to store result data identifying at least addressed data in which malware was not found;

wherein said addressed data is cached when it has been retrieved.

20. (Cancelled)

21. (Original) Apparatus as claimed in claim 19, wherein said address identifying logic is operable to search within said currently held data for string data having a format matching a pointer to an internet address.

22. (Original) Apparatus as claimed in claim 19, wherein said currently held data includes received e-mail messages.

23. (Original) Apparatus as claimed in claim 19, wherein said scanning logic is operable to seek to detect within said addressed data one or more of:

computer viruses;

worms;

Trojans;

banned computer programs;

banned words; or

banned images.

24. (Original) Apparatus as claimed in claim 19, wherein said computer is a firewall computer via which internet traffic is passed to a local computer network.

25. (Cancelled)

26. (Original) Apparatus as claimed in claim 19, wherein if malware is detected within said addressed data, then one or more malware found actions are triggered.

27. (Original) Apparatus as claimed in claim 19, wherein said malware found actions including at least one of:

(i) preventing access to said currently held data;

(ii) removing said at least one internet address from said currently held data;

(iii) preventing access to said addressed data;

(iv) removing said malware from said addressed data to generate clean addressed data and supplying said clean addressed data in place of said addressed data;

(v) blocking internet access by a computer detected to be seeking to access said at least one internet address.

28. (New) A computer program product as claimed in claim 1, wherein said currently held data is an e-mail and said internet address is an internet link embedded in said e-mail.

29. (New) A computer program product as claimed in claim 1, wherein said currently held data is a file and said internet address is an internet link embedded in said file.

30. (New) A computer program product as claimed in claim 8, wherein said malware found actions include removing said at least one internet address from said currently held data.

31. (New) A computer program product as claimed in claim 1, wherein addressed data determined to contain malware via said scan is cleaned and said clean addressed data is stored locally for access via said internet address.

32. (New) A computer program product as claimed in claim 1, wherein access to said addressed data is allowed if said result data associated with said addressed data identifies said addressed data as not containing malware and if said addressed data has not changed since it was last scanned.